Remarks

In the Office Action dated September 7, 2005, the Examiner rejected claims 1-4, 8-11, 13-16, and 20-23 under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent to Bahlmann 6,487,594 in view of U.S. Patent to Brownlie et al. (Brownlie) 6,202,157. Examiner rejected claims 5-7, 12, 17-19, and 24 under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent to Bahlmann 6,487,594 in view of U.S. Patent to Brownlie et al. (Brownlie) 6,202,157 and in further view of Moriconi et al. (Moriconi) 6,158,010. Claims 5, 12, 17, and 24 are cancelled. Claims 25-31 are new.

With regard to amended claims 1 and 13, Moriconi does not disclose, teach, or suggest a method and system for verifying that the policy instance complies with the policies. Moriconi's local policy is "based on," *i.e.*, derived from, its global security policy and is not an independent input into the system. (Moriconi, col. 4, lines 20-24.) Applicants' local policy is independent of its global policy. (Figure 1.) Thus, if Mariconi's local and global policies were reconciled, using the methods described by Applicants, then the compliance checking of claims 1 and 13 will always succeed. Applicants' invention, however, allows a participant to have a local policy that was not previously reconciled or previously derived from global policy. In that case, Applicants' local policy can be checked for compliance with a policy instance. For example, a local policy could require a 512 bit encryption key length while the policy instance could require a 1024 bit encryption key length. In that case, the compliance checking of claims 1 and 13 could warn the participant that the policy instance in force is not compliant with the participant's local policy. Moriconi teaches away from verifying that the policy instance complies with the policies because Moriconi's local policy—which is derived from its global policy—can never be in non-compliance with its global policy. (Moriconi, col. 4, lines 20-24.)

With regard to independent claims 1 and 13, Bahlmann does not disclose, teach, or suggest a method and system for determining security policy for a group of participants. Bahlmann, instead, refers to the provisioning of devices within the Internet. (Bahlmann, col.

1, lines 59-63, col. 2, lines 64-65.) Furthermore, Bahlmann merely suggests that policy is retrieved through a hierarchy of servers. (Bahlmann, col. 1, lines 59-63, col. 2, lines 64-65.)

With regard to claims 1 and 13, Bahlmann does not disclose, teach, or suggest generating a policy instance that applies to the group based on the group and local polices wherein the policy instance defines a configuration of services used to implement a session. Bahlmann merely discusses a hierarchy of servers being repositories for policy, which are then given to individual servers. Bahlmann performs no reconciliation of subsequent analysis. (Bahlmann, col. 2, lines 8-12 and lines 34-36.)

For at least these reasons, claims 1 and 13 are patentable.

Claims 2-4, 6-11, 13-16, and 18-23 depend directly or indirectly from claims 1 and 13 respectively. For at least the reasons claims 1 and 13 are patentable, claims 2-4, 6-11, 13-16, and 18-23 are patentable. Claims 2-4, 6-11, 13-16, and 18-23 include additional limitations making them further patentable.

With regard to claims 3 and 15, Brownlie does not disclose, teach, or suggest a method and system wherein the step of analyzing verifies that the policy instance adheres to a set of principles defining legal construction and composition of the security policy. Brownlie validates the policy by checking its digital signature, *i.e.*, Brownlie validates the source of the policy. (Brownlie, col. 5, lines 33-37.) Applicants, in contrast, validate the content of the policy, *e.g.*, Applicants validate the meaning of the policy.

With regard to claims 8 and 20, Brownlie does not disclose, teach, or suggest, a method and system wherein the step of enforcing includes the steps of creating and processing events. With regard to claims 10 and 22, Brownlie does not disclose, teach, or suggest a method and system wherein the step of creating events includes the step of translating application requests into the events. Brownlie discusses the format and meaning of policy rules in the stated environment: ". . . policy I.D. should obtain in the event that an overriding or underriding policy is subsequently published." (Brownlie, col. 6, lines 33-55.) Brownlie uses the term "event" to mean "in the occurrence that," whereas Applicants use the term "event," for example, to mean a physical signaling message between policy components. The subjects of claims 8, 10, 20, and 22 and the cited Brownlie text are unrelated.

With regard to claims 9 and 21, Brownlie does not disclose, teach, or suggest a method and system wherein the step of enforcing includes delivering the events to security services via a real or software-emulated broadcast bus. Brownlie discusses the exchange of policies between network nodes via a secure communication method. (Brownlie, col. 7, lines 58-64.) Secure communication methods for data between two nodes are well known and include the work cited by Brownlie. The real or software-emulated broadcast bus of claims 9 and 21 is for event delivery within a machine for various service components that enforce the policy. (Page 33, lines 1-10.) Each mechanism decides whether the even can be processed by that mechanism and consults the Policy Engine to decide if event processing is allowed and what action to take on the event. (Page 36, lines 21-25; Page 37, lines 1-6.)

With regard to claims 11 and 23, Brownlie does not disclose, teach, or suggest a method and system wherein the step of enforcing further includes the steps of creating and processing timers and messages. Brownlie discusses the use of initialization messages with periodic updates within the context of the distribution of policies to nodes, (Brownlie, col. 7, lines 50-56), not the enforcement of polices.

With regard to claims 6 and 18, Brownlie does not disclose, teach, or suggest a method and system comprising identifying parts of a local policy that are not compliant with the policy instance and determining modifications required to make the local policy compliant with the policy instance. Brownlie merely teaches the selection of policy based on a policy ID that allows different applications to use different policies by associating different Policy ID's with different applications. (Brownlie, col. 7., lines 41-49.)

With regard to claims 7 and 19, Brownlie does not disclose, teach, or suggest a method and system comprising preventing a potential participant from participating in the session if the policy instance does not comply with the set of local requirements of the potential participant. Brownlie discusses the selection of rules to enforce in order to prevent an unauthorized action, *e.g.*, accessing a resource. (Brownlie, col. 7, lines 12-14.) Claims 7 and 19 are directed to two sets of policies, *e.g.*, a local policy and a policy instance, and allows a participant to determine if the two policies are compliant: the inputs to Applicants' invention are two policies. Brownlie teaches away from Applicants' invention because the inputs to Brownlie are the rules to enforce a policy and an action, *e.g.*, accessing a resource.

Applicants believe the claims are in a condition for allowance. Applicants request a notice to that effect. Applicants also invite a telephone conference if the Examiner believes it will advance the prosecution of this application.

Please charge any additional fees or credit any overpayment as a result of the filing of this paper to our Deposit Account No. 02-3978. A duplicate of this paper is enclosed for that purpose.

Respectfully submitted,

PATRICK D. MCDANIEL, ET AL.

By____________________
Benjamin C. Stasa,
Reg. No. 55,644
Attorney for Applicants

Date: 11/7/05

BROOKS KUSHMAN P.C.
1000 Town Center, 22nd Floor
Southfield, MI 48075-1238
Phone: 248-358-4400
Fax: 248-358-3351